(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 471 038 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
17.04.2019 Bulletin 2019/16

(51) Int Cl.:
G06Q 20/32 *(2012.01)* ***G06Q 20/36*** *(2012.01)*
G06Q 20/38 *(2012.01)*

(21) Application number: **17196489.3**

(22) Date of filing: **13.10.2017**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(71) Applicant: **Mastercard International Incorporated**
Purchase NY 10577 (US)

(72) Inventors:
- **HAY, Florent**
  1090 Jette (BE)
- **CHEN, Kuan Hua**
  London, KT2 5DT (GB)
- **ROBERTS, David Anthony**
  Warrington, WA4 5RD (GB)

(74) Representative: **Lawrence, Richard Anthony**
Keltie LLP
No.1 London Bridge
London SE1 9BA (GB)

(54) USER AUTHENTICATION AND TRANSACTION STAGING

(57) There is presented a method and a computing device for user authentication and transaction staging on a user device. The method comprises authenticating a user of the user device by a first device verification method and generating transaction credentials at the user device. The method further comprises generating at least one optical code data corresponding to the transaction credentials and displaying the at least one optical code on the user device in a form suitable for scanning by a second device to progress a transaction with the second device.

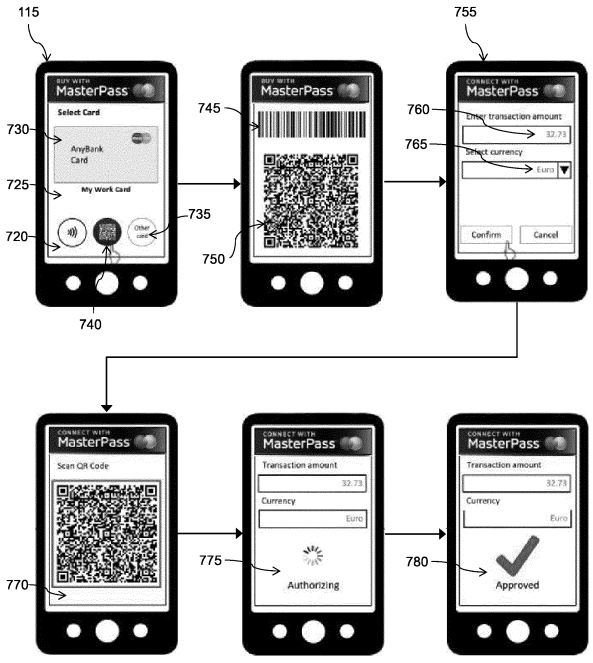


Figure 7

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The present disclosure relates to user authentication and transaction staging particularly, but not exclusively, on a computing device. Aspects of the disclosure relate to a method and a computing device.

BACKGROUND

[0002] It is now commonplace to conduct payment transactions electronically such as by using, for example, a debit card, a credit card or an electronic wallet on a mobile device. Two main types of electronic payment transactions currently dominate the payments industry when using debit or credit cards: magnetic-stripe transactions and Europay, MasterCard and Visa (EMV) transactions. Magnetic-stripe transactions involve using a card that is capable of storing data on a band of magnetic material the magnetic stripe on the card. To perform a magnetic-stripe transaction, the payment card is swiped into a terminal by a cardholder.

[0003] There are two categories of EMV transactions: contact transactions and contactless transactions. Contact EMV transactions, like magnetic-stripe transactions, require that the card be in contact with the terminal for the transaction to occur. In contrast, contactless transactions rely on near field communication (NFC) technology. To perform a contactless EMV transaction, the payment card is tapped against a terminal by the cardholder when prompted to do so.

[0004] Typically, a payment transaction performed using an electronic wallet (e-wallet) application uses NFC technology to provide payment credentials from an electronic device to a merchants point-of-sale (POS) terminal. At present there are several issues with using NFC for performing payment transactions.

[0005] Firstly, the users electronic device and the merchants POS terminal must both be compatible with NFC technology for the transaction to be performed. There are many electronic devices that are not compatible with NFC such as, for example, Apples iPhone up to and including iPhone 5S. More recent models of Apple s iPhone, such as from the iPhone 6 up to and including iPhone 7 plus, include NFC capability; however the NFC capability of these iPhone models is exclusive to ApplePay and cannot be accessed by e-wallets other than ApplePay. Although contactless mobile payments are becoming more popular, not all merchants are able to accept NFC payments as they would require a compatible card reader, which may for some merchants be more expensive requiring the introduction of a POI device in comparison with the ease of reusing an already present barcode reader.

[0006] Alongside NFC technology, some e-wallets support the use of one-dimensional or two-dimensional barcode technology, for example Quick Response Code (QRC) is an example of a two-dimensional barcode, to perform electronic payment transactions. The main advantage of using QRC technology for making payments is ubiquity any smartphone is capable of installing the software required for displaying a QRC and any smartphone equipped with a camera is capable of installing the software required for reading a QRC. Further, performing a transaction by QRC is quick, easy and convenient for the user.

[0007] There are, however, issues with current methods of payment by QRC. For example, currently when using QRC for payment transactions, both the merchant and the user are required to have a data connection. In addition, the scanning of the QRC for performing a payment transaction is not guaranteed to function on every occasion. Further, there are issues with the security of the payment transaction. For example, the unidirectional nature of QR means that it is not possible for the terminal to participate in the security of the cryptogram generation hence an alternative means to ensure freshness is needed.

[0008] Therefore there is scope for improvement on current methods of electronic payments. The present disclosure has been devised to mitigate or overcome at least some of the above-mentioned problems.

SUMMARY OF THE DISCLOSURE

[0009] According to an aspect of the present disclosure there is provided a computer-implemented method of user authentication and transaction staging on a user device. The method comprises authenticating a user of the user device by a first device verification method and generating transaction credentials at the user device. The method further comprises generating at least one optical code data corresponding to the transaction credentials and displaying the at least one optical code on the user device in a form suitable for scanning by a second device to progress a transaction with the second device.

[0010] Each of the at least one optical code may be a barcode.

[0011] An electronic wallet may be opened before generating transaction credentials on the user device.

[0012] A payment card may be selected from one or more payment cards associated with the electronic wallet to be used for the transaction.

[0013] Transaction information may be entered at the user device and the transaction information may be included in the at least one barcode.

[0014] The at least one barcode may comprise a one-dimensional barcode and a two-dimensional barcode. At least the two-dimensional barcode may be displayed.

[0015] The barcode data may comprise formatted transaction data.

[0016] The method may further comprise generating at a processor of the user device one or more unpredictable numbers for a transaction, and using the unpredictable numbers to generate the at least one barcode.

[0017] The one-dimensional code may be generated using formatted Dynamic Magstripe data, and the two-dimensional code may be generated using formatted EMV data and formatted Dynamic Magstripe data.

[0018] The transaction credentials may be time-limited.

[0019] The transaction credentials may be authenticated by the merchant using EMV combined data authentication to place an asymmetric cryptogram in the barcode.

[0020] The transaction credentials may be generated by the user device without requiring input by the user.

[0021] The method may further comprise receiving a notification with the transaction credentials at the user device for corroboration of the transaction by the user.

[0022] According to an aspect of the present disclosure there is provided a computing device adapted for user authentication and transaction staging, comprising at least one processor and at least one memory and an electronic wallet application. The computing device is adapted to authenticate a user of the device by a method of verification. The device is adapted further to generate transaction credentials and generate at least one optical code data corresponding to the transaction credentials. Further the device is adapted to display the at least one optical code on the computing device in a form suitable for scanning by a second device to progress a transaction with the second device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] One or more embodiments of the disclosure will now be described, by way of example only, with reference to the accompanying drawings, in which like components are assigned like numerals and in which:

Figure 1 illustrates schematically the relevant components of an electronic wallet platform for enabling electronic payment transfers in accordance with an embodiment of the disclosure;

Figure 2 shows schematically the relevant parts of the exemplary hardware architecture for a mobile computing device suitable for implementing an embodiment of the disclosure;

Figure 3 illustrates the software architecture of a mobile computing device, in accordance with an embodiment of the disclosure;

Figure 4 illustrates schematically method steps in a general embodiment of the disclosure;

Figure 5 illustrates schematically method steps in a first embodiment of the disclosure;

Figure 6 illustrates schematically method steps in a second embodiment of the disclosure;

Figure 7 illustrates a mobile device adapted for authenticating and performing a transaction in accordance with a third embodiment of the disclosure;

Figure 8 illustrates a mobile device adapted for authenticating and performing a transaction in accordance with a fourth embodiment of the disclosure;

Figure 9 shows a sequence diagram for authenticating and performing a transaction on a user device in accordance with an embodiment of the disclosure;

Figure 10 illustrates the method *generateMchipUN()* for returning an unpredictable number for an M/Chip QRC transaction in accordance with an embodiment of the disclosure;

Figure 11 illustrates the data elements used in the generation of the byte array for an M/Chip QRC transaction, in accordance with an embodiment of the disclosure;

Figure 12 illustrates the method *generateMagstripeUN()* for returning an unpredictable number for a Magstripe QRC transaction in accordance with an embodiment of the disclosure;

Figure 13 shows a point-of-interaction (POI) processing decision tree for an EMV-QRCPS M/Chip transaction, in accordance with an embodiment of the disclosure;

Figure 14 comprises a table indicating the layout of the Track 2 Equivalent Data that is processed in order to process a M/Chip transaction; and

Figure 15 illustrates a typical four-party model used in payment interactions between entities operating in a card scheme.

DETAILED DESCRIPTION

[0024] The claimed method provides a payment solution that uses optical code scanning and is integrated into an application.

[0025] The approach taken to performing an electronic payment involves using an electronic wallet to make more secure and convenient payment transactions. The claimed method involves generating and displaying an optical code comprising the payment transaction credentials on a user device. The optical code may be a non-complex graphic sign that contains encoded information, such as an optical glyph, or a one-dimensional or multi-dimensional barcode. Once the optical code is displayed, it can be scanned by a merchant device to perform a payment transaction. If, however, a near-field communication (NFC) signal is detected, an NFC contactless payment may take priority over the scanning of the optical

code to perform a payment transaction. For example, if an NFC signal is detected, the optical code may be removed from the screen and a regular contactless payment transaction may be performed.

[0026] The optical code displayed on the user device may be a one-dimensional (1-D) barcode, such as a Code 128 barcode or any code that uses a series, or a two-dimensional barcode (2-D), such as a Quick Response Code (QR Code or QRC). The specific embodiments described in detail below use 1-D and 2-D barcodes, but as the skilled person will appreciate different forms of optical code may be employed as discussed above. Multiple barcodes may be displayed on the user device which enables the merchant to select which barcode to scan depending on their terminal capabilities. Optionally, the user may enter information about the transaction such as, for example, the transaction amount, the currency and/or the country in which the transaction is performed, prior to the generation of the barcode(s). The transaction information may be embedded in the barcode and used in the generation of a cryptogram.

[0027] The user device and the merchant device used in the claimed disclosure may be any form of electronic device, but the claimed disclosure has particular utility for mobile computing devices such as smart phones, and relevance to applications such as mobile banking.

[0028] General and specific embodiments of the disclosure will be described below with reference to the Figures.

[0029] Figure 15 is a schematic block diagram of a typical four-party model or four-party payment transaction scheme. The diagram illustrates the entities present in the model and the interactions occurring between entities.

[0030] Normally, card schemes payment networks linked to payment cards are based on one of two models: a three-party model (adopted by American Express) or a four-party model (adopted by Visa and Mastercard). For the purposes of this document, the four-party model is described in further detail below.

[0031] The four-party model may be used as a basis for the transaction network. For each transaction, the model comprises four entity types: cardholder (1610), merchant (1620), issuer (1630) and acquirer (1640). In this model, the cardholder (1610) purchases goods or services from the merchant (1620). The issuer (1630) is the bank or any other financial institution that issued the card to the cardholder (1610). The acquirer (1640) provides services for card processing to the merchant (1620).

[0032] The model also comprises a central switch (1650) interactions between the issuer (1630) and the acquirer (1640) are routed via the switch 1650). The switch (1650) enables a merchant (1620) associated with one particular bank (acquirer (1640)) to accept payment transactions from a cardholder (1610) associated with a different bank (issuer (1630)).

[0033] A typical transaction between the entities in the four-party model can be divided into two main stages: authorisation and settlement. The cardholder (1610) initiates a purchase of a good or service from the merchant (1620) using their card. Details of the card and the transaction are sent to the issuer (1630) via the acquirer (1640) and the switch (1650) to authorise the transaction. Should the transaction be considered abnormal by the issuer (1630), the cardholder (1610) may be required to undergo a verification process to verify their identity and the details of the transaction. Once the verification process is complete the transaction is authorised.

[0034] On completion of the transaction between the cardholder (1610) and the merchant (1620), the transaction details are submitted by the merchant (1620) to the acquirer (1640) for settlement.

[0035] The transaction details are then routed to the relevant issuer (1630) by the acquirer (1640) via the switch (1650). Upon receipt of these transaction details, the issuer (1630) provides the settlement funds to the switch (1650), which in turn forwards these funds to the merchant (1620) via the acquirer (1640).

[0036] Separately, the issuer (1630) and the cardholder (1610) settle the payment amount between them. In return, a service fee is paid to the acquirer (1640) by the merchant (1620) for each transaction, and an interchange fee is paid to the issuer (1630) by the acquirer (1640) in return for the settlement of funds.

[0037] Figure 1 illustrates schematically the relevant components of an electronic wallet (e-wallet) platform (100) for enabling electronic payment transfers in accordance with an embodiment of the disclosure. The e-wallet platform comprises three main components, namely an e-wallet service provider (105) (e.g. a payment network provider such as Mastercard or a mobile network operator), an electronic device (115) (e.g. a mobile computing device such as a smart phone), and an e-wallet software application (135) or customer application installed on the electronic device (e.g. Masterpass or Android Pay). The e-wallet platform (100) also comprises one or more networks (110) to enable the transfer of data between the service provider (105) and the electronic device (115), as well as the payer, the payee and their respective banks. A user of the electronic device can use the combination of components in the e-wallet platform to make and receive payment transactions.

[0038] Figure 2 shows schematically the relevant parts of the exemplary hardware architecture for a mobile computing device (115) suitable for implementing an embodiment of the disclosure. In the example shown, the mobile computing device is a mobile cellular telecommunications handset (mobile phone or mobile device) in other embodiments, the computing device may be another type of computing device such as a laptop computer or a tablet and the computing device need not have cellular telecommunications capabilities. The mobile phone (115) has a display (120) providing, in this example, a touch-screen user interface. The mobile phone (115) is equipped with a wireless telecommunications apparatus

(125) for communication with a wireless telecommunications network and local wireless communication apparatus (130).

[0039] Figure 3 illustrates the software architecture (300) of a mobile computing device (115), in accordance with an embodiment of the disclosure. In Figure 3, a main operating environment (305) of the mobile computing device is shown along with a protected operating environment (340). The protected operating environment (340) may be a Subscriber Identity Module (SIM), Universal Integrated Circuit Card (UICC), a Secure Element or a hardware backed Trusted Execution Environment. Alternatively, there may be a sandbox or other logically protected environment in the main operating environment to provide a secure environment.

[0040] The main operating environment (305) comprises an application processor (310) and associated memories (315). The main operating environment may be used with a generic operating system (such as iOS or Android). The main operating environment also comprises other applications normally needed by such a mobile computing device, such as a browser (320), a modem (325) and a camera driver (330).

[0041] The protected operating environment (340) may comprise an e-wallet software application (135). Alternatively, the elements relevant to the security of the e-wallet software application may be comprised in the protected operating environment. In Figure 3, an e-wallet software application (135) is shown explicitly in the protected operating environment (340). The application may be located within the SIM (305) or within another physically or logically protected environment. Alternatively, some parts of the mobile payment application may be situated in the protected operating environment. Further, data from the application may be located in a protected memory.

[0042] Figure 4 illustrates schematically method steps in a general embodiment of the disclosure for authenticating and performing a transaction on a user device. First of all, the method comprises opening (410) an e-wallet application on a user device. The described embodiments are applicable to any form of e-wallet, also known as a digital wallet or a mobile wallet, and may be implemented using various electronic devices, such as tablets, desktop computers, laptop computers as well as mobile phones. After opening the e-wallet application, the user is authenticated (420) by a consumer device cardholder verification method. This provides the assurance that the correct cardholder is performing the transaction. A consumer device cardholder verification method (CDCVM) is a method of cardholder verification in which the credentials associated with the user are entered directly into the user device and not via a merchant device. Such consumer device cardholder verification methods may include a personal identification number (PIN), a password, biometric authentication mechanisms such as a fingerprint or an iris scan. Once the user has been authenticated, the user is able to initiate a payment transaction via the e-wallet application user interface in order to purchase goods or services. Payment transaction credentials are generated (430). Prior to processing the transaction, the method may ensure that no other contactless transaction is performed simultaneously. Alternatively, the payment transaction credentials may be authenticated by the merchant by putting an asymmetric cryptogram (EMV CDA combined data authentication) in the QR code, for example using an Elliptic Curve version of CDA.

[0043] The next step of the method is generating (440) a barcode comprising the payment transaction credentials. The method may generate a one-dimensional (1-D) barcode, a two-dimensional (2-D) barcode, or both a 1-D barcode and a 2-D barcode at the same time. Advantageously, if a merchant is unable to scan the 2-D barcode, for example, due to barcode scanner limitations, they can attempt to scan the 1-D barcode to process the transaction. First, the transaction information and terminal information may be retrieved and queried to determine whether or not the transaction is allowed. The user device may receive the transaction information and terminal information out-of-band, before the generation of the barcodes, which would avoid any need for manual entry of this information by the user.

[0044] Dynamic magstripe data (DMSD) and EMV data may be generated simultaneously by the e-wallet application. DMSD, which in turn comprises a cryptogram calculated based on a time stamp, is provided in the 1-D barcode, whereas both DMSD and EMV data are provided in the 2-D barcode. An advantage of providing both types of transaction data in the 2-D barcode is that if a merchant is able to scan a 2-D barcode but is unable to perform an EMV transaction, for example, due to network limitation, the merchant can attempt to perform a DMSD transaction by scanning the 2-D barcode. A DMSD transaction provides a higher level of security than using static track data. In the example in Figure 4, the method focusses on generating a 2-D barcode comprising the payment transaction credentials and displaying the 2-D barcode on the user device.

[0045] As described above, both DMSD and EMV data are generated and provided in the 2-D barcode. For the generation of EMV data, the method returns one or more unpredictable numbers for the transaction, given the date and time. An unpredictable number is a value created for each transaction to provide variability and uniqueness to the generation of a cryptogram. The purpose of an unpredictable number is mainly to ensure that the data is fresh . In other words, to provide some confidence that it was generated at the time of the transaction and in conjunction with the POI at which the transaction is performed. Because barcode technologies are unidirectional the usual process as described in EMV of getting a value from the terminal and including it in the device s calculation of a cryptogram subsequently returned to the POI is not easy to do.

[0046] Whilst another solution such as scanning a bar-

code from the terminal and subsequently generating a barcode for the terminal might be performed, or using a handover to another technology, or using a parallel comms channel such as modulated light or sound may provide such a channel, a simpler solution that is more reliable for the participants is adopted in DMSD generation. For the generation of DMSD, the method encodes time in lieu of the unpredictable number. The method then carries out a cryptogram calculation, based on the obfuscated time procedure, which may be carried in Track 2 data.

[0047] The method then returns a structure comprising two sets of formatted transaction data: one set according to EMV-QRC; and the other according to DMSD. The returned structure may also comprise a Transaction ID specific to the barcode. The Transaction ID may be used to reconcile the payment with the transaction details. The returned structure is then used in the generation of a 2-D barcode.

[0048] Once generated, the 2-D barcode is displayed (450) on the user device to be scanned (460) by a merchant device. The user may receive a notification with the payment transaction credentials at the user device to enable the user to corroborate the payment transaction. A payment transaction is then performed (470). The final step is receiving (480) a transaction delivery notification on the user device.

[0049] Figure 5 illustrates schematically method steps in a first embodiment of the disclosure. The first step in this embodiment is opening (510) an e-wallet application on a user device. After opening the e-wallet application, there is an authentication step to authenticate (520) the user by a consumer device cardholder verification method. In the e-wallet, the user is prompted to select (530) a payment card to be used for the payment transaction.

[0050] There is configurable information in the e-wallet to indicate whether only a 2-D barcode should be returned by the method or whether both a 1-D barcode and a 2-D barcode should be returned by the method. While use of a 2-D barcode will generally be preferred if supported by all parties as a 2-D barcode can carry a significant amount of information allowing a full transaction protocol to be used, some parties may only support 1-D barcode scanning. In these cases a 1-D solution may be used. Once a payment card has been selected and the barcode type has been indicated (540), the e-wallet generates (550) payment transaction credentials on the user device.

[0051] The next step of the method is generating the barcode(s) comprising the payment transaction credentials. First, the transaction information may be retrieved and queried to determine whether or not the transaction is allowed.

[0052] In the present embodiment, the user is indicating (540) that 1-D and 2-D barcodes should both be displayed on the screen of the user device. DMSD and EMV data is generated simultaneously by the e-wallet application. DMSD, which in turn comprises a cryptogram calculated based on a time stamp, is provided in the 1-D barcode, whereas both DMSD and EMV data are provided in the 2-D barcode.

[0053] For the generation of EMV data, the method returns one or more unpredictable numbers for the transaction, given the date and time. For the generation of DMSD, the method encodes time in lieu of the unpredictable number. The method then carries out a cryptogram calculation, based on the obfuscated time procedure, which may be carried in Track 2 data.

[0054] The method then returns a structure comprising two sets of formatted transaction data: one set according to EMV-QRC which is used in the generation of a 2-D barcode; and the other according to DMSD which is provided in both the 1-D barcode and the 2-D barcodes. The Transaction ID may be used to reconcile the payment with the transaction details. This structure is then used in the generation of a 2-D barcode.

[0055] Next, a 1-D barcode and a 2-D barcode are both displayed (570) on the screen of the user device. In this example, the merchant is equipped with a 1-D barcode scanner but is not able to scan 2-D barcodes. The merchant, therefore, scans (580) the 1-D barcode with the 1-D barcode scanner.

[0056] Following the scanning of the barcode, a payment transaction is performed (590). The final step is receiving (595) a transaction delivery notification on the user device.

[0057] The present disclosure enables two ways of conveying payment data, each providing a different level of security. It is advantageous from the perspective of acceptance coverage for the merchant to be able to select whether to scan a 1-D barcode or a 2-D barcode depending on the type of barcode scanner available to the merchant at the time. Merchants who have a 1-D barcode scanner would be unable to scan a 2-D barcode however they would be able to scan the 1-D barcode instead and proceed to perform a transaction. In addition, in the event that the 2-D barcode fails to scan, the 1-D barcode may be used to perform the payment transaction.

[0058] Figure 6 illustrates schematically method steps in a second embodiment of the disclosure. The first three steps namely, (610), (620) and (630) are equivalent to the first three steps of the first embodiment described in Figure 5. These first three steps involve opening (610) an e-wallet application, authenticating (620) the user, and selecting (630) a payment card to be used for the payment transaction.

[0059] The user may then be prompted to enter (640) payment transaction credentials such as, for example, the transaction amount and/or the currency of the transaction. In some cases the user may enter the transaction amount but may not enter the currency of the transaction; in this case the currency code may be set to null. The format of the inputted credentials may then be validated.

[0060] The user may also be prompted to indicate whether only a 2-D barcode should be returned by the

method or whether both a 1-D barcode and a 2-D barcode should be returned by the method. Once a payment card has been selected, the transaction credentials entered (640), and the barcode type indicated (650), the e-wallet generates (660) payment transaction credentials on the user device.

[0061] The next step of the method is generating the barcode(s) comprising the payment transaction credentials. First, the transaction information may be retrieved and queried to determine whether or not the transaction is allowed. Given the system date and time, the method may return one or more unpredictable numbers for a transaction.

[0062] In the present embodiment, the user is indicating (650) that only a 2-D barcode should be displayed on the screen of the user device. In this example, within the method step of generating (670) a 2-D barcode comprising the payment transaction credentials, an unpredictable number for an EMV-QRC transaction is returned. This unpredictable number is used in the calculation of an application cryptogram. The method then returns a structure comprising a single set of formatted transaction data according to EMV-QRC which allows the generation of a 2-D barcode.

[0063] When generating a barcode, errors may be encountered if, for example: one or more input parameter has an incorrect format; the transaction is declined due to the user not be authenticated or another reason; there are no payment transaction credentials available for the transaction; or an error is encountered during cryptographic operations.

[0064] Next, a 2-D barcode is displayed (680) on the screen of the user device. In this example, a merchant device is able to scan (690) the 2-D barcode. Following the scanning of the barcode, a payment transaction is performed (685) and a transaction delivery notification is received (695) by the user device upon successful completion of the transaction.

[0065] Figure 7 illustrates a mobile device (115) adapted for authenticating and performing a transaction in accordance with a third embodiment of the disclosure. This embodiment is described with reference to an e-wallet application (720), such as, for example, Masterpass, which may be installed on a mobile device (115). The e-wallet application (720) is the e-wallet application component of an e-wallet platform for enabling electronic payment transfers on an electronic device wherein the payment network provider is Mastercard. The user of the mobile device can use the combination of components in the e-wallet platform to make and receive payment transactions.

[0066] Firstly, the e-wallet application (720) may be opened and displayed on a screen of the device (115) by a user. Once the application is opened, the user may be presented with a payment card selection page (725) on which one or more payment cards (730) such as, for example, credit or debit cards that can be used to make a payment transaction may be displayed. The user may also be presented with an option to select a card that is not currently displayed on the payment card selection page (725). This option may be accessible through an Other card icon (735) on the screen. The user may then be prompted to select a payment card to be used for the payment transaction. The user may respond by either selecting a payment card (730) on the payment card selection page (725) or a different payment card through the Other card icon (730). The user may then then indicate, via a barcode indication icon (740), that both a 1-D barcode and a 2-D barcode should be returned by the application and displayed on the screen.

[0067] Once a payment card has been selected and the barcode type has been indicated, the e-wallet may generate payment transaction credentials and generate the barcodes comprising the payment transaction credentials. A 1-D barcode (745) and a 2-D barcode (750) are then both displayed on the screen.

[0068] Payment transaction credentials such as, for example, the transaction amount (760) and the currency (765) of the transaction may be entered into a merchant POS application on a merchant device (755). As another option, the user may enter the payment transaction credentials before the barcodes are generated.

[0069] In this case, the merchant device is capable of scanning 2-D barcodes. The 2-D barcode is scanned (770) by the merchant device and, subsequently, the transaction is performed (775). Once the transaction has been performed successfully, a transaction delivery notification (780) is displayed on the mobile device.

[0070] Figure 8 illustrates a mobile device (115) adapted for authenticating and performing a transaction in accordance with a fourth embodiment of the disclosure.

[0071] The e-wallet application (720) may be opened and displayed on a screen of the device (115) by a user. Once the application is opened, the user may be presented with a payment card selection page (725) on which one or more payment cards (730) such as, for example, credit or debit cards that can be used to make a payment transaction may be displayed. The user may also be presented with an option to select a card that is not currently displayed on the payment card selection page (725). This option may be accessible through an Other card icon (735) on the screen. The user may then be prompted to select a payment card to be used for the payment transaction. The user may respond by either selecting a payment card (730) on the payment card selection page (725) or a different payment card through the Other card icon (735). The user may then then indicate, via a barcode indication icon (740), that both a 1-D barcode and a 2-D barcode should be returned by the application and displayed on the screen.

[0072] Once a payment card has been selected and the barcode type has been indicated, the e-wallet may generate payment transaction credentials and generate the barcodes comprising the payment transaction credentials. A 1-D barcode (745) and a 2-D barcode (750) are then both displayed on the screen.

[0073] Payment transaction information such as, for example, the transaction amount (760) and the currency (765) of the transaction are entered into a merchant POS application on a merchant device (755). As another option, the user may enter the payment transaction credentials before the barcodes are generated.

[0074] In this case, the merchant device is not capable of scanning 2-D barcodes. Instead, the merchant is equipped with a 1-D barcode scanner (870). The merchant, therefore, scans the 1-D barcode (745) with the 1-D barcode scanner (870).

[0075] Subsequently, the transaction is performed (875). Once the transaction has been performed successfully, a transaction delivery notification (880) is displayed on the mobile device.

[0076] Figure 9 shows a sequence diagram for authenticating and performing a transaction on a user device in accordance with an embodiment of the disclosure. Figure 9 illustrates an exemplary embodiment of the general embodiment discussed in Figure 4.

[0077] This embodiment is described with reference to a payment transaction performed with a payment from a consumer to a merchant. Exemplary classes that may be used for performing the transaction using MasterPass are described below.

[0078] First, the consumer (902) opens (904) the e-wallet application which appears on the user interface (906) of the consumers mobile device. After opening e-wallet, the consumer is verified by a consumer device cardholder verification method (CDCVM). A user authentication request (908) is submitted to a CDCVM Manager (910). The consumer is informed once they have been authenticated (912) successfully.

[0079] The consumer (902) then initiates a payment transaction by selecting an icon termed *Pay with QR-Code* (914) on the user interface of the mobile device. Optionally, the consumer may enter the transaction amount and/or the currency of the transaction (916) via the user interface (906).

[0080] A class named *MchipEngine* (918) comprises a method called *processQrcTransaction* (920). The method *processQrcTransaction* (920) takes an entity class, *QrcInputData,* and returns an entity class, *QrcOutputData* (922), comprising formatted data to generate a QRC, as well as a Transaction ID specific to each barcode.

[0081] When the method *processQrcTransaction* (920) is processed, *MchipEngine* (918) may perform a format check (924) of the input data provided in the *QrcInputData* structure. Next, the transaction information and terminal information may be retrieved and queried to determine whether or not the transaction is allowed. If the transaction is allowed, the *QrcOutputData* (922) structure is built and returned. *QrcOutputData* (922) comprises EMV-QRC (M/Chip) data and optionally Dynamic Magstripe Data.

[0082] The *QrcInputData* structure may, for example, comprise the amount of the transaction, the currency of the transaction, and/or the country code of the transaction (916). Prior to processing a QRC transaction, *MchipEngine (918)* may ensure that no contactless transaction is being performed simultaneously.

[0083] *MagstripeQrc* is a class responsible for providing dynamic Magstripe data. The method *generateMagstripeUN()* (926) returns an unpredictable number for a Magstripe QRC transaction, given the system date and time. Using a byte array representing the generated unpredictable number and a parameter of type *KeyType*, the method *computeCvc3* (928) computes and returns a card verification code (CVC3) cryptogram.

[0084] CVC3 is a type of card security code used for the purpose of minimising fraud in payment card transactions when the card is not physically present. The code is a three or more digit number that is a dynamic variant of the one that appears at the back of the card (CVC1). CVC3 is calculated at each contactless or QRC magstripe transaction. The card security code may also be known as, for example, the card verification data (CVD), card verification value (CW) or signature panel code (SPC).

[0085] The formatted Track 2 data is then returned (930), which contains Dynamic CVC3. *MagstripeQrc* then builds the object *MagstripeQrcData* (932) which comprises dynamic Magstripe data and optionally a Transaction ID for the present transaction.

[0086] *MchipQrc* is a class responsible for providing input data to allow the terminal to build formatted transaction data according to EMV-CPS which allows the generation of a 2-D barcode. *MchipQrc* may also retrieve a Transaction ID for the present transaction. The method *generateMchipUN()* (934) returns an unpredictable number for an M/Chip QRC transaction given access to the system date and time. Using a byte array representing the generated unpredictable number and a parameter of type *KeyType*, the method *computeApplicationCryptogram* (936) computes and returns an application cryptogram. Chip data is then returned and converted into an appropriate encoding scheme, in this case Base64 (938). *MchipQrc* then builds the object *MchipQrcData* (940) which comprises EMV-QRC (M/Chip) data and optionally a Transaction ID for the present transaction.

[0087] The *QrcOutputData* (922) structure is built and returned. In this example, *QrcOutputData* (922) comprises both EMV-QRC (M/Chip) data (in *MchipQrcData*) and Dynamic Magstripe Data (in *MagstripeQrcData*). The data is then sent to a *library that generates barcodes* (942) for code generation. For 1-D barcode generation, the *MagstripeQrcData* component of *QrcOutputData* (922) is sent to a *library that generates barcodes* (942), which then returns a 1-D barcode (944). For 2-D barcode generation, the *MchipQrcData* component of *QrcOutputData* (922) is sent to a *library that generates barcodes* (942), which then returns a 2-D barcode (946). Both the 1-D barcode and the 2-D barcode are then displayed (948) in the user interface (906).

[0088] Either the 1-D barcode or the 2-D barcode may

be scanned (950) by a merchant device a decision that would depend on the type of device available to the merchant and the type of barcode that may be scanned by the available merchant device. A payment transaction is then performed (952). Once the application has been performed, a transaction delivery notification (954) is sent from the MasterCard Digital Enablement Service (MDES) (956), which corresponds to the MasterCard digitisation and tokenisation platform, to the user interface (906).

[0089] Figure 10 illustrates the method *generateMchipUN()* for returning an unpredictable number for an M/Chip QRC transaction in accordance with an exemplary embodiment of the disclosure.

[0090] The method *generateMchipUN()* (1000) must be able to access the system date and time. The time may be the number of minutes since a starting point of the system. In order to mask the time value and make it transaction specific, it is obfuscated.

[0091] An example of the method *generateMchipUN()* in use will now be described with reference to Figure 10. First, the current device time as elapsed time since a defined starting point is obtained (1002). This time is then converted (1004) into the elapsed number of minutes. Next, a Primary Account Number (PAN), an Application Transaction Counter (ATC) and a domain identifier are concatenated (1006) and hashed (1008). The PAN is not the cardholders real account number used by the issuer to fund the transaction but rather the tokenized value and taken as a compressed numeric value. The ATC is a sequential counter, usually internal to a chip application, that is maintained by the payment application. The ATC is incremented by the payment application each time the application is executed. The length of the ATC is normally 2 bytes. The domain identifier is a value provided to each program by Mastercard that consists of a variable number of bytes of data. The length of the domain identifier may be from zero bytes upwards.

[0092] Then, the least significant (rightmost) 4 bytes of the concatenation result is taken (1010) as an integer. Of this 4-byte integer, the least significant 8 bits would correspond to the last byte of the 4-byte integer. The sum (1012) of the time in elapsed number of minutes and the hashed 4-byte integer results in a 4-byte array that represents the unpredictable number (1014).

[0093] Thus, the output of the method *generateMchipUN()* (1000) is a byte array, consisting of 4 bytes, that is used as an unpredictable number (1014) in the calculation of the Application Cryptogram. The 4-byte array representing the unpredictable number is then used (1016) by the method *computeApplicationCryptogram* (936) to compute and return an Application Cryptogram for an M/Chip QRC transaction.

[0094] An M/Chip QRC transaction is based on a Digital Secure Remote Payment (DSRP) transaction with time in place of the unpredictable number and with the payment device generating the complete set of data to the terminal so that it may construct the authorisation request.

[0095] Figure 11 illustrates the data elements used in the generation of the byte array for an M/Chip QRC transaction, in accordance with an exemplary embodiment of the disclosure.

[0096] As described above, EMV-QRC (M/Chip) formatted transaction data enables the generation of a 2-D barcode. In order to build the M/Chip data, a byte array representing an unpredictable number is generated. The byte array may be generated by concatenating a Tag (1102) and a Value (1104) of the data elements shown in Figure 11. Referring to Figure 11, the Application Version Number has a value assigned by Mastercard and is used by Mastercard to indicate the format and content within the Application Specific Transparent Template.

[0097] Figure 12 illustrates the method *generateMagstripeUN()* for returning an unpredictable number for a Magstripe QRC transaction in accordance with an exemplary embodiment of the disclosure.

[0098] In the method *generateMagstripeUN()* (1200), a UN may be generated by the mobile device. The time value, or time stamp, generated by the mobile device may be used as the UN for the generation of the CVC3 cryptogram.

[0099] An example of the method *generateMagstripeUN()* (1200) in use will now be described with reference to Figure 12.

[0100] First, a time stamp is generated (1202) by the mobile device at the time of a transaction. The time stamp may be a number based on the hour and/or minute and/or second and/or date of the transaction. This time stamp may be utilised (1204) as the UN for a transaction. The UN is utilised to generate (1206) the CVC3 and the ATC for use in authentication processing.

[0101] Upon receipt of the CVC3 value or cryptogram during authentication processing, the authentication system re-computes (1208) the CVC3 and compares it to the value received. If the UN provided by the mobile device is within a predetermined threshold amount or range of the time stamp provided by the merchants POS terminal for the transaction, the authorisation system validates (1210) that the time stamp is current.

[0102] The UN or time stamp is obfuscated and made transaction dependent so that a potential thief cannot easily observe or make use of the time value.

[0103] It should be noted that in some embodiments, the mobile device may be configured to generate a number for use as the UN that is not based on a time stamp or time value. The mobile device may be configured to perform a cryptographic calculation to generate the CVC3 cryptogram for a particular transaction based on a cryptographic key, the generated UN as described above, a transaction count value, and static data stored on the mobile device.

[0104] Figure 13 shows a point-of-interaction (POI) processing decision tree (1400) for an EMV-QRC M/Chip transaction, in accordance with an embodiment of the disclosure.

[0105] POI transactions may be EMV-QRC (M/Chip) transactions or magnetic-stripe card-based payment transactions (Magstripe).

[0106] The first step is to check whether or not the payment product is supported (1402) (EMV-QRC). In this example, the selected payment product is M/Chip Digital QRC. A positive result proceeds to the next step, which is to check whether or not the mandatory POI data is present (1404). If the payment product is not supported, the POI throws an exception (1406). If the mandatory POI data is present (1408), the POI checks if the transparent data is present. If the mandatory POI data is missing, the POI throws an exception (1410). If the transparent data is not present, the POI proceeds to process a Magstripe transaction (1114). It the transparent data is present (1412), the format of the transaction data is determined if the format is recognised (1416), the POI then checks if the mandatory transparent data is present; if the format is not recognised (1418), the POI proceeds to process a Magstripe transaction. Further, if the mandatory transparent data is missing (1422), the POI proceeds to process a Magstripe transaction. Given the presence of the mandatory transparent data (1420), the POI proceeds to process the M/Chip transaction (1424).

[0107] To process the M/Chip transaction, the Track 2 Equivalent Data (tag 57) is processed. Track 2 Equivalent Data must be provided in the OR Code and contains the data objects of the Track 2. Track 2 Equivalent Data has a maximum length of 37 positions. Figure 14 comprises a table indicating the layout of the Track 2 Equivalent Data, which comprises the data field (1502), length (1504) and the format (1506).

[0108] The Track 2 Equivalent Data is processed by first extracting the PAN (1508) and Expiration Date (1510) components of the Track 2 Data and storing them as corresponding EMV data: Application PAN and Application Expiration Date. The issuer s specified restrictions on the geographic use and services allowed for the application is then checked. The transaction record is then built for authorisation.

[0109] The completion (1426) of a transaction involves transaction disposition. The POI is responsible for indicating the transaction disposition to the cardholder, which is from an authorisation response. A receipt is printed once the transaction is completed. In addition, the POI may be required to display POI messages, perform merchant specific processing and/or process additional data.

[0110] Further embodiments of the disclosure may be provided in accordance with the scope of the disclosure as defined here.

Claims

1. A computer-implemented method of user authentication and transaction staging on a user device, the method comprising:

   authenticating (420) a user of the user device by a first device verification method;

   generating (430) transaction credentials at the user device;

   generating (440) at least one optical code data corresponding to the transaction credentials;

   displaying (450) the at least one optical code on the user device in a form suitable for scanning by a second device to progress a transaction with the second device.

2. The method of Claim 1, wherein each of the at least one optical code is a barcode.

3. The method of Claim 1, further comprising opening (410) an electronic wallet before generating transaction credentials on the user device.

4. The method of Claim 3, further comprising selecting a payment card to be used for the transaction from one or more payment cards associated with the electronic wallet.

5. The method of any preceding claim, further comprising entering transaction information at the user device and including said transaction information in the at least one barcode.

6. The method of any preceding claim, wherein said at least one optical code comprises a one-dimensional barcode and a two-dimensional barcode, and wherein at least the two-dimensional barcode is displayed.

7. The method of any preceding claim, further comprising generating at a processor of the user device one or more unpredictable numbers for a transaction, and using the unpredictable numbers to generate the at least one barcode.

8. The method of Claim 5, wherein the one-dimensional code is generated using formatted Dynamic Magstripe data, and wherein the two-dimensional code is generated using formatted EMV data and formatted Dynamic Magstripe data.

9. The method of any preceding claim, wherein the transaction credentials are time-limited.

10. The method of any preceding claim, wherein the transaction credentials are received by the user device without requiring input by the user.

11. The method of any preceding claim, wherein the method further comprises receiving a notification with the transaction credentials at the user device for corroboration of the transaction by the user.

12. A computing device adapted for user authentication

and transaction staging, comprising at least one processor and at least one memory and an electronic wallet application, wherein the computing device is adapted to:

authenticate (420) a user of the device by a method of verification;
generate (430) transaction credentials;
generate (440) at least one optical code data corresponding to the transaction credentials; and
display (450) the at least one optical code data on the computing device in a form suitable for scanning by a second device to progress a transaction with the second device.

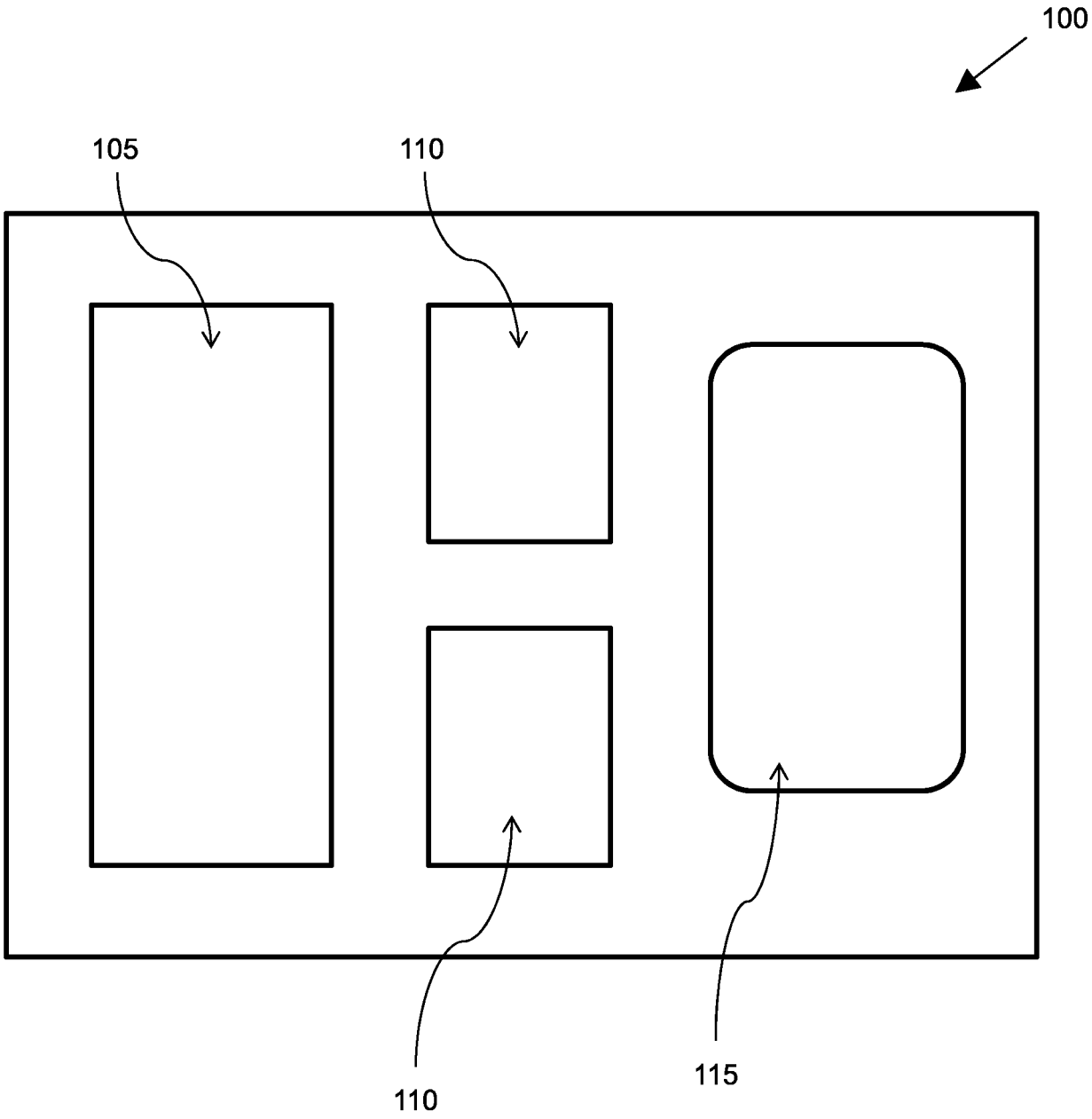


Figure 1

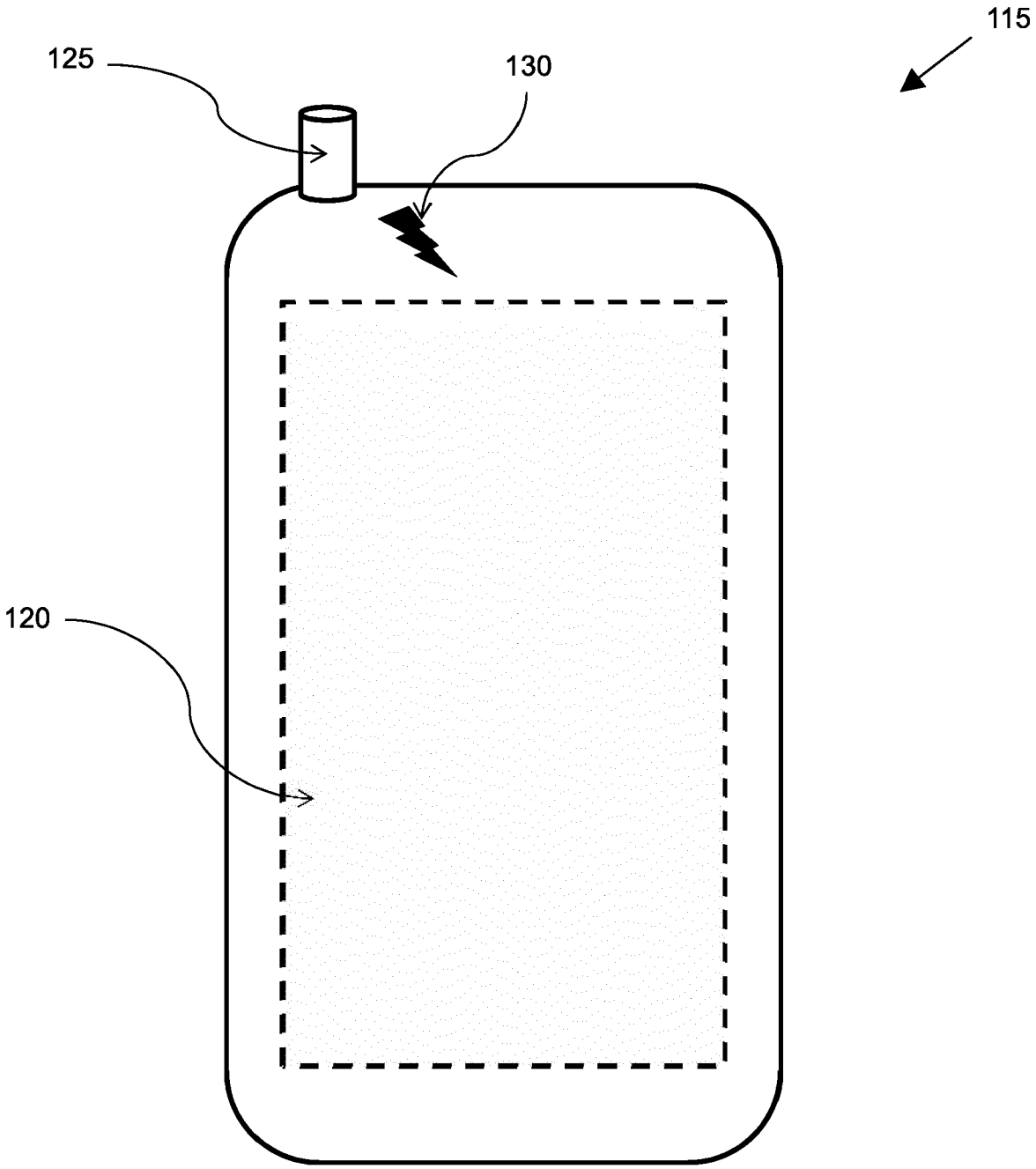


Figure 2

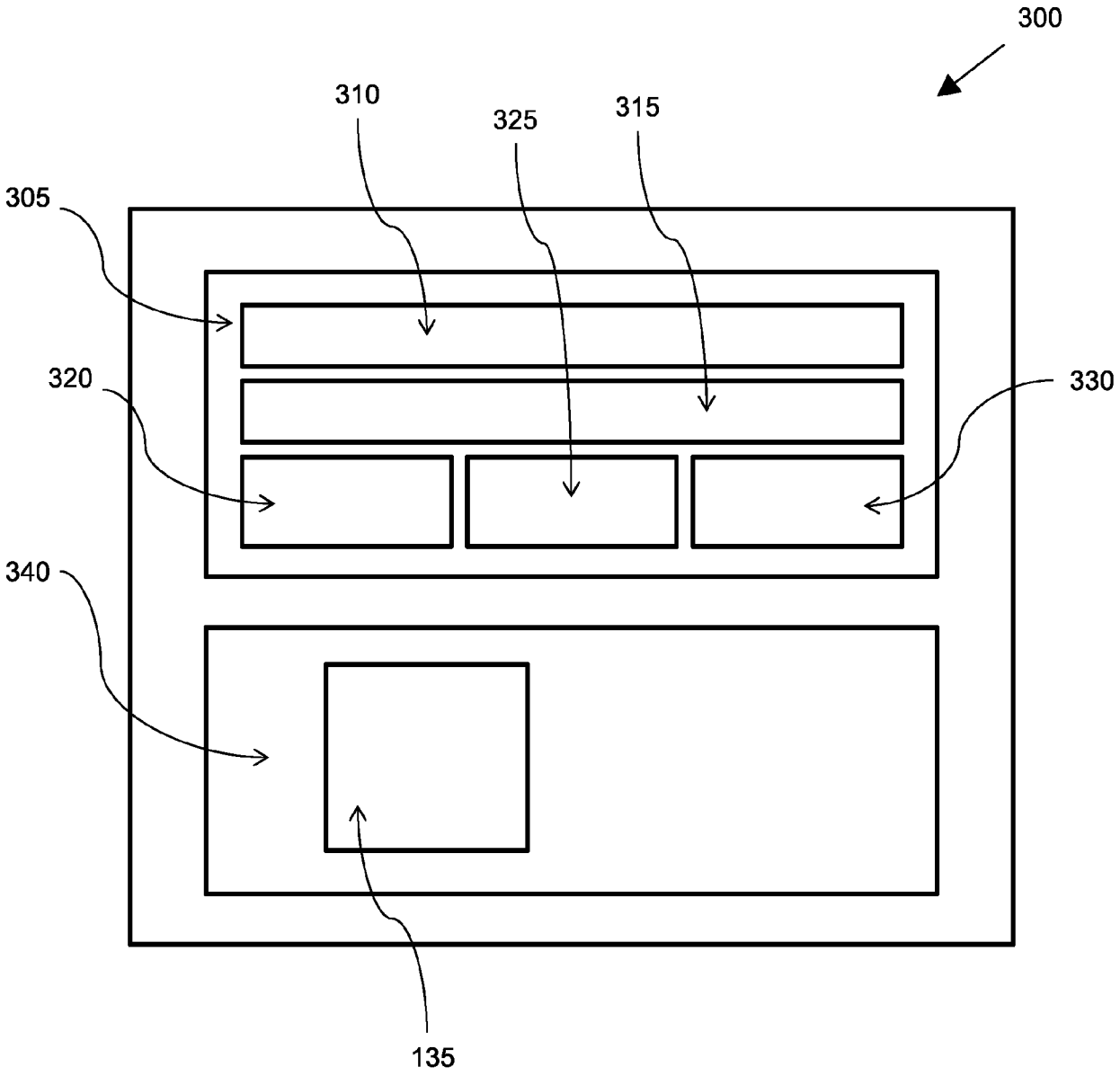


Figure 3

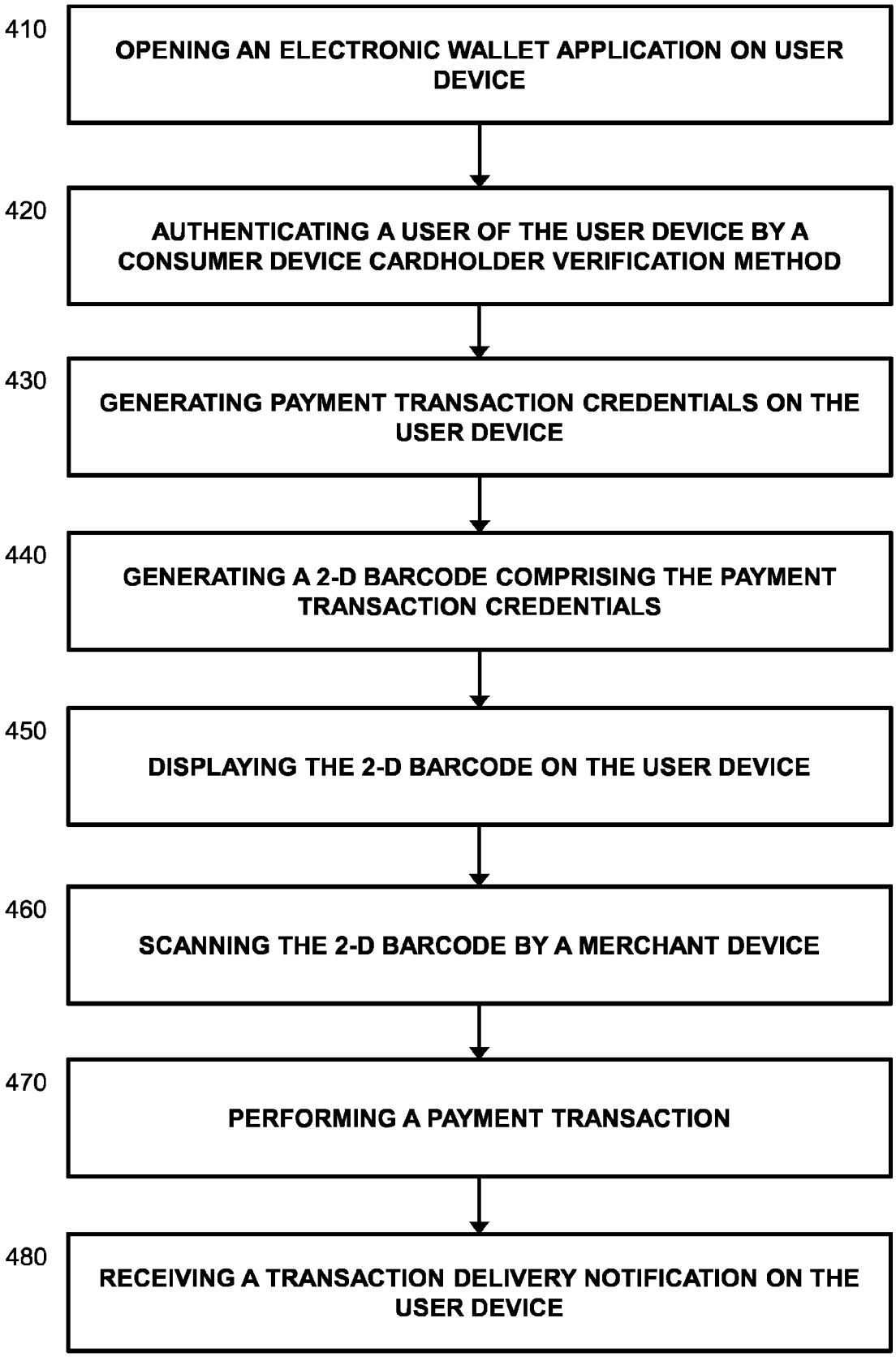

410
OPENING AN ELECTRONIC WALLET APPLICATION ON USER DEVICE
420
AUTHENTICATING A USER OF THE USER DEVICE BY A CONSUMER DEVICE CARDHOLDER VERIFICATION METHOD
430
GENERATING PAYMENT TRANSACTION CREDENTIALS ON THE USER DEVICE
440
GENERATING A 2-D BARCODE COMPRISING THE PAYMENT TRANSACTION CREDENTIALS
450
DISPLAYING THE 2-D BARCODE ON THE USER DEVICE
460
SCANNING THE 2-D BARCODE BY A MERCHANT DEVICE
470
PERFORMING A PAYMENT TRANSACTION
480
RECEIVING A TRANSACTION DELIVERY NOTIFICATION ON THE USER DEVICE

Figure 4

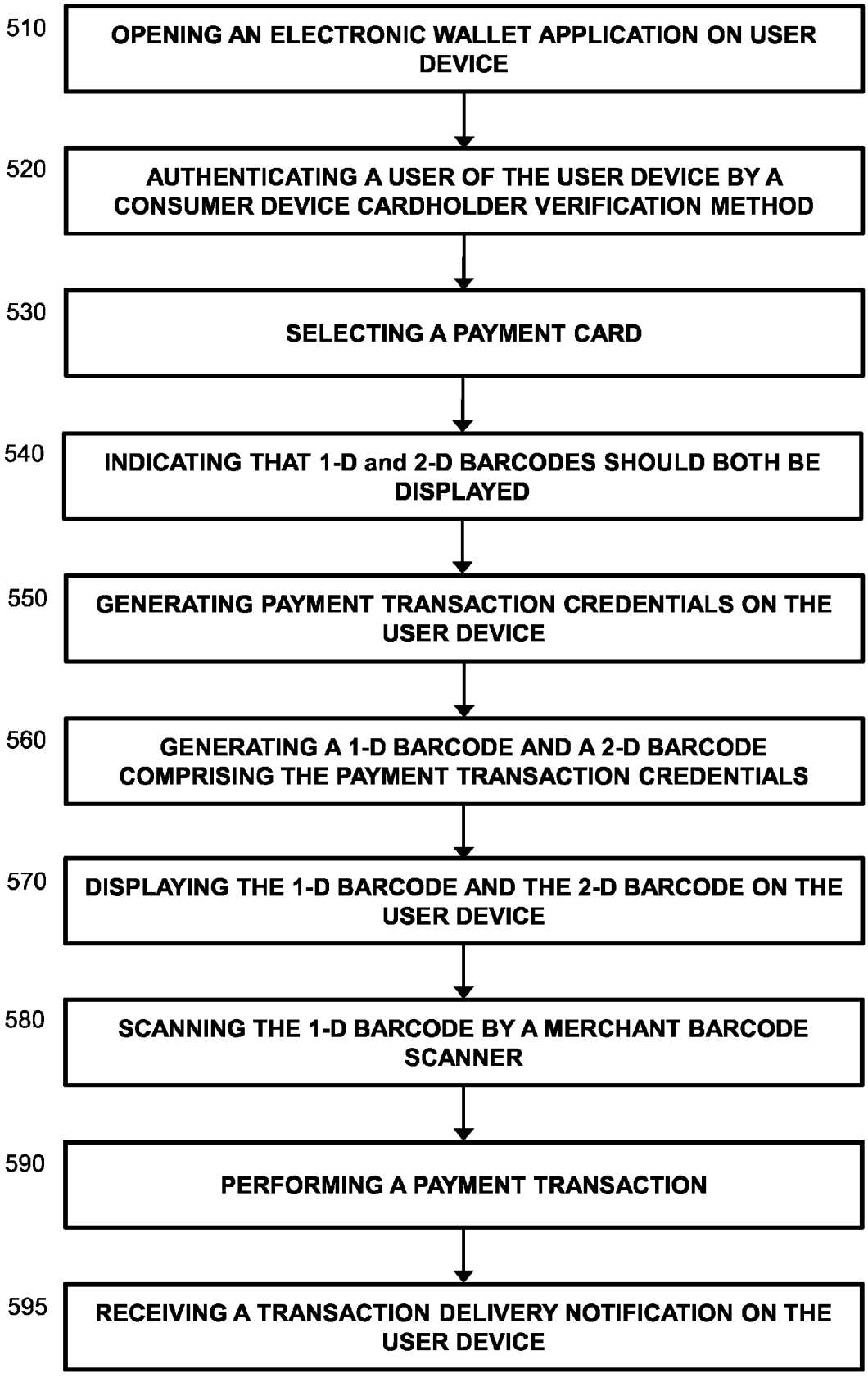

510
OPENING AN ELECTRONIC WALLET APPLICATION ON USER DEVICE
520
AUTHENTICATING A USER OF THE USER DEVICE BY A CONSUMER DEVICE CARDHOLDER VERIFICATION METHOD
530
SELECTING A PAYMENT CARD
540
INDICATING THAT 1-D and 2-D BARCODES SHOULD BOTH BE DISPLAYED
550
GENERATING PAYMENT TRANSACTION CREDENTIALS ON THE USER DEVICE
560
GENERATING A 1-D BARCODE AND A 2-D BARCODE COMPRISING THE PAYMENT TRANSACTION CREDENTIALS
570
DISPLAYING THE 1-D BARCODE AND THE 2-D BARCODE ON THE USER DEVICE
580
SCANNING THE 1-D BARCODE BY A MERCHANT BARCODE SCANNER
590
PERFORMING A PAYMENT TRANSACTION
595
RECEIVING A TRANSACTION DELIVERY NOTIFICATION ON THE USER DEVICE

Figure 5

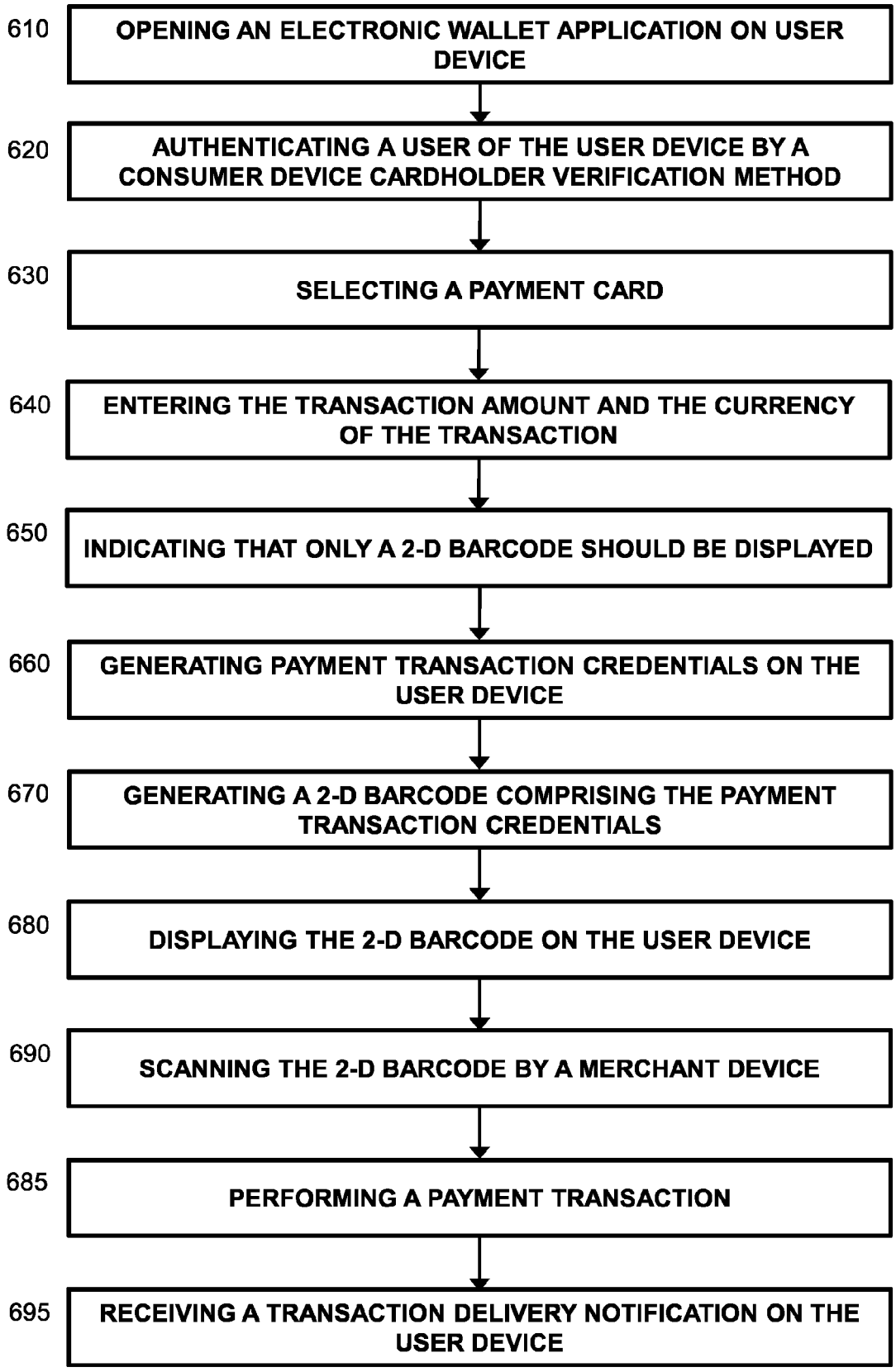

610
OPENING AN ELECTRONIC WALLET APPLICATION ON USER DEVICE
620
AUTHENTICATING A USER OF THE USER DEVICE BY A CONSUMER DEVICE CARDHOLDER VERIFICATION METHOD
630
SELECTING A PAYMENT CARD
640
ENTERING THE TRANSACTION AMOUNT AND THE CURRENCY OF THE TRANSACTION
650
INDICATING THAT ONLY A 2-D BARCODE SHOULD BE DISPLAYED
660
GENERATING PAYMENT TRANSACTION CREDENTIALS ON THE USER DEVICE
670
GENERATING A 2-D BARCODE COMPRISING THE PAYMENT TRANSACTION CREDENTIALS
680
DISPLAYING THE 2-D BARCODE ON THE USER DEVICE
690
SCANNING THE 2-D BARCODE BY A MERCHANT DEVICE
685
PERFORMING A PAYMENT TRANSACTION
695
RECEIVING A TRANSACTION DELIVERY NOTIFICATION ON THE USER DEVICE

Figure 6

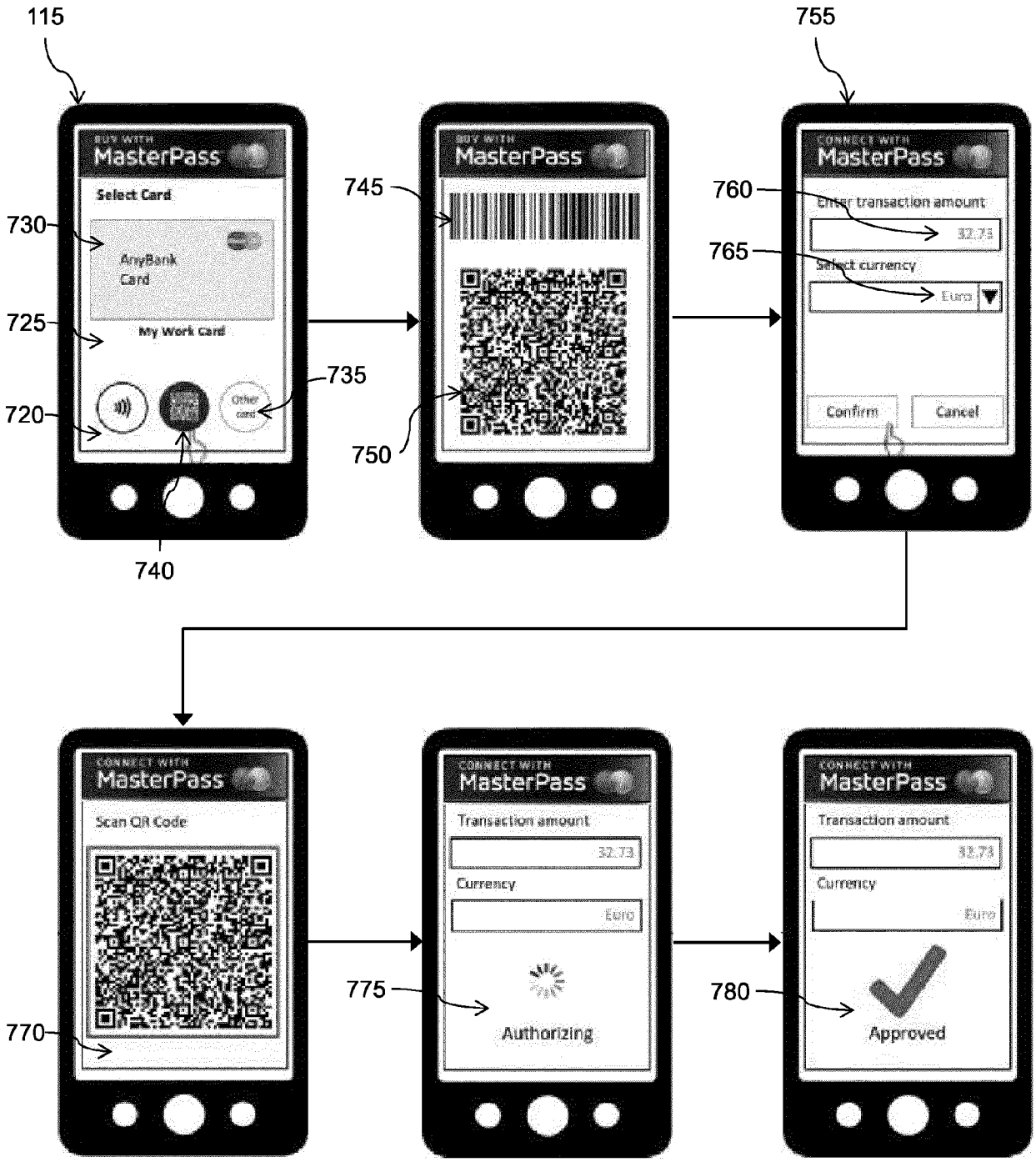

115
755
730
745
760
765
725
735
720
750
740
770
775
780
BUY WITH MasterPass
Select Card
AnyBank Card
My Work card
Other card
CONNECT WITH MasterPass
Enter transaction amount
32.73
Select currency
Euro
Confirm
Cancel
Scan QR Code
Transaction amount
Currency
Authorizing
Approved

Figure 7

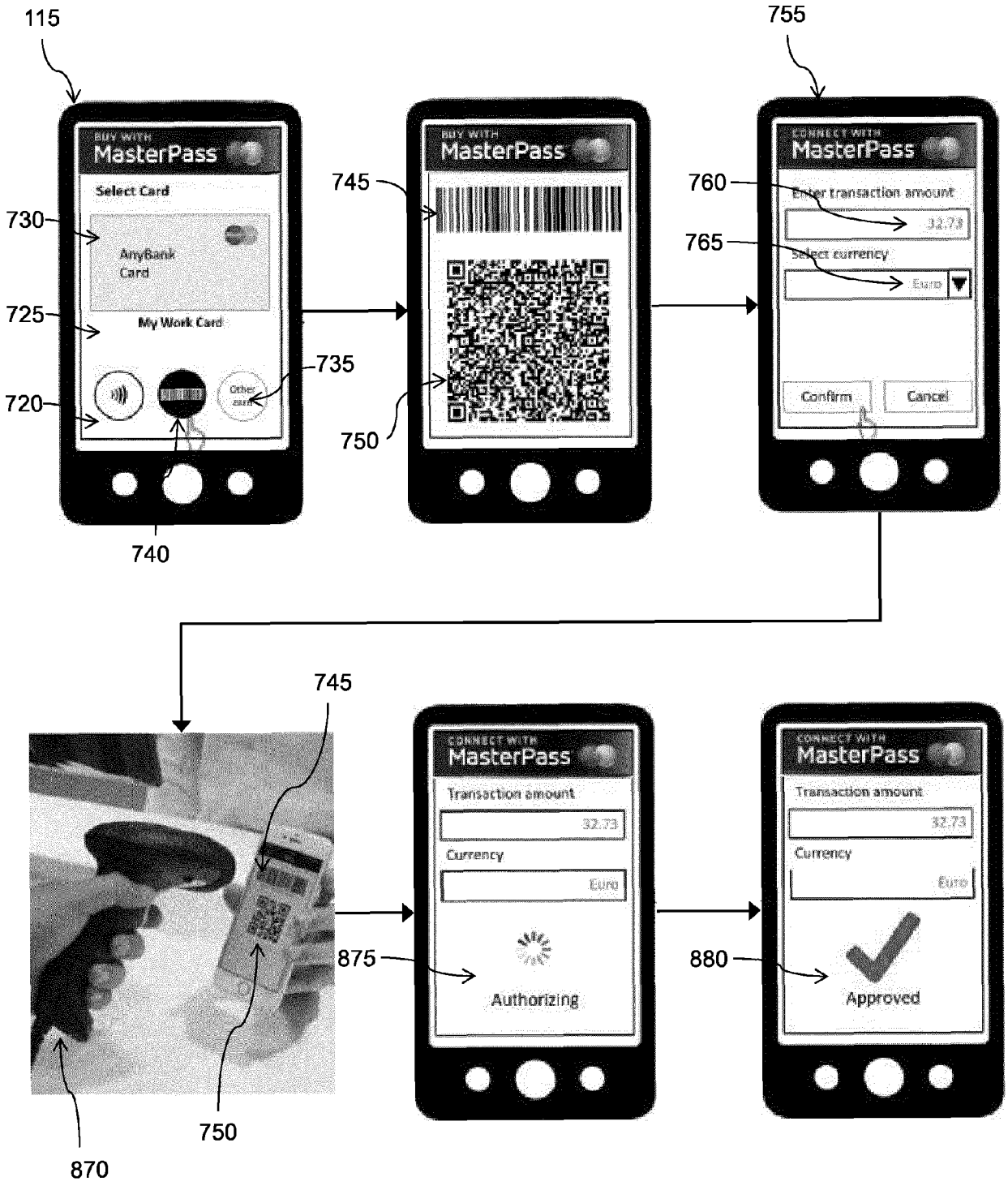

115
755
BUY WITH MasterPass
Select Card
AnyBank Card
My Work Card
730
725
720
735
740
745
750
760
765
CONNECT WITH MasterPass
Enter transaction amount
32.73
Select currency
Euro
Confirm
Cancel
745
750
870
875
880
Transaction amount
Currency
Authorizing
Approved

Figure 8

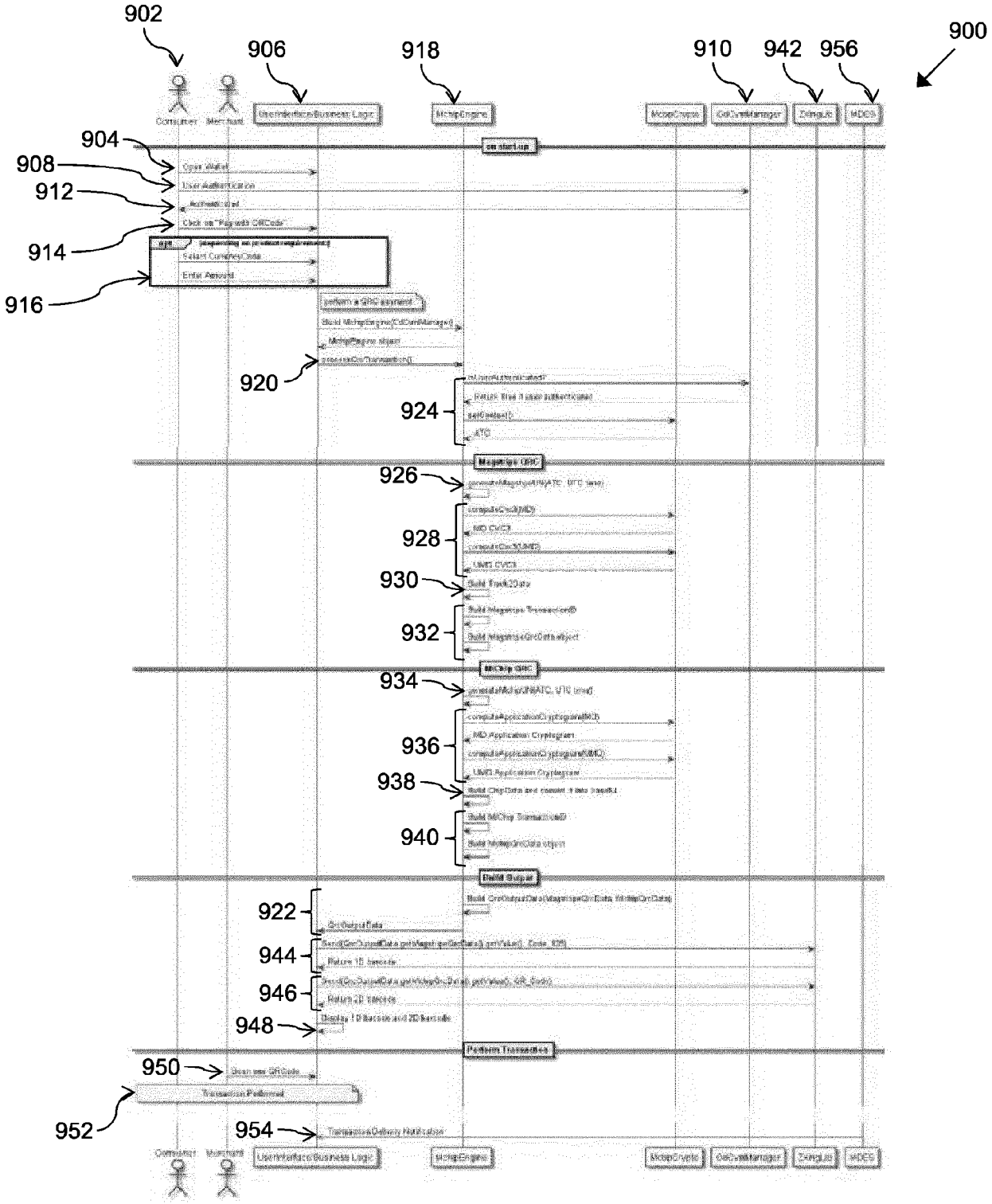

902
906
918
910
942
956
900
904
908
912
914
916
920
924
926
928
930
932
934
936
938
940
922
944
946
948
950
952
954

Figure 9

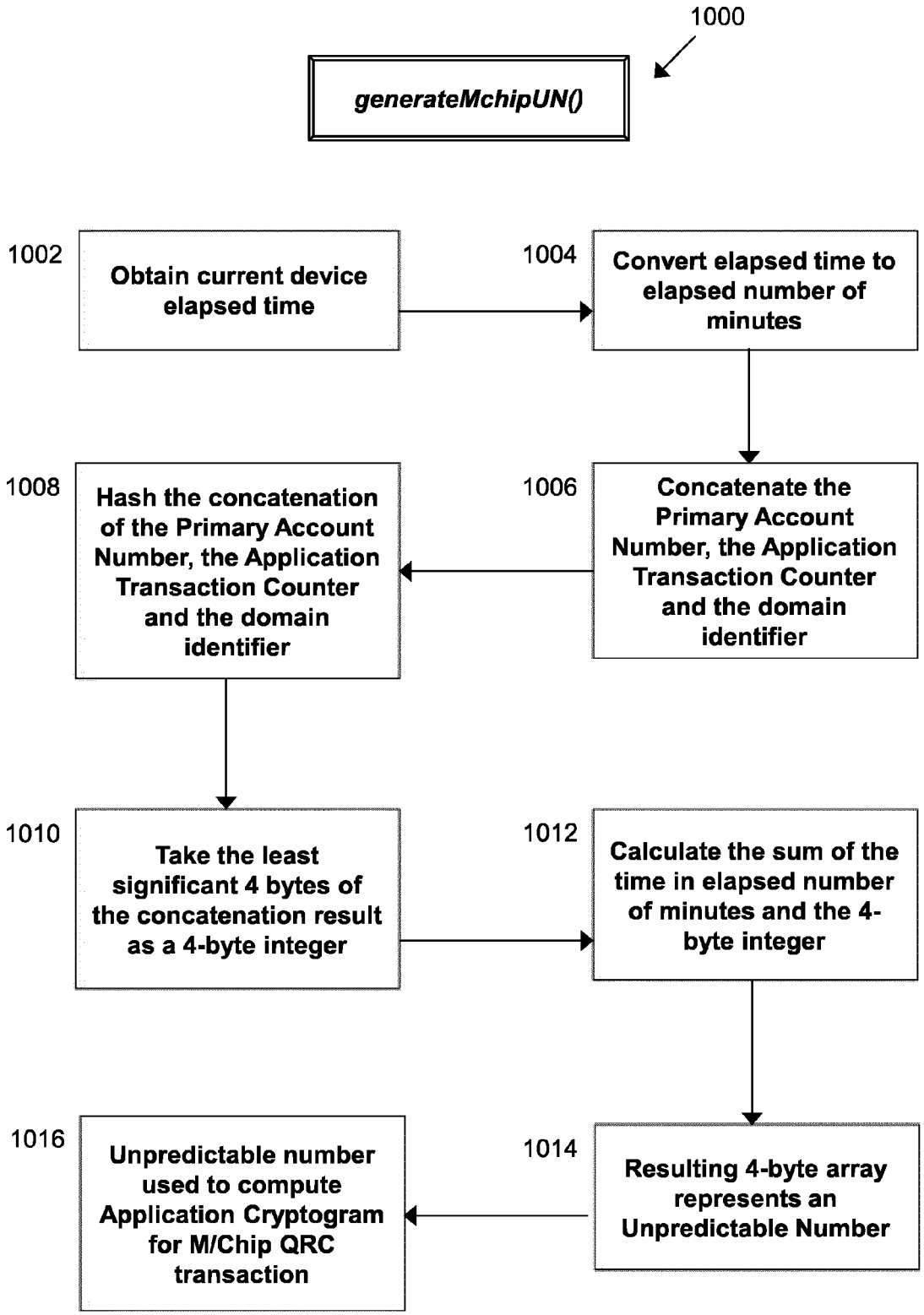

1000
generateMchipUN()
1002
Obtain current device elapsed time
1004
Convert elapsed time to elapsed number of minutes
1006
Concatenate the Primary Account Number, the Application Transaction Counter and the domain identifier
1008
Hash the concatenation of the Primary Account Number, the Application Transaction Counter and the domain identifier
1010
Take the least significant 4 bytes of the concatenation result as a 4-byte integer
1012
Calculate the sum of the time in elapsed number of minutes and the 4-byte integer
1014
Resulting 4-byte array represents an Unpredictable Number
1016
Unpredictable number used to compute Application Cryptogram for M/Chip QRC transaction

Figure 10

1102 1104

Tag	Value			Format	Presence
'61'	Application Template			bytes	M
	'4F'	Application Definition File (ADF) Name (AID)		bytes	M
	'50'	Application Label		bytes	M
	'57'	Track 2 Equivalent Data		bytes	M
	'9F24'	Payment Account Reference		bytes	O
	'9F25'	Last 4 Digits of PAN		byte	O
	'9F08'	Application Version Number		bytes	M
	'5F20'	Cardholder Name		bytes	O
	'5F2D'	Language Preference		bytes	O
	'9F19'	Token Requestor ID		bytes	O
	'63'	Application Specific Transparent Template		bytes	M
		'9F07'	Application Usage Control	bytes	M
		'9F11'	Issuer Code Table Index	byte	O
		'9F12'	Application Preferred Name	bytes	O
		'9F26'	Application Cryptogram	bytes	M
		'9F10'	Issuer Application Data	bytes	M
		'9F36'	Application Transaction Counter	bytes	M
		'95'	Terminal Verification Results	Bytes	O
		'9F27'	Cryptogram Information Data	byte	M
		'9F34'	CVM Results	bytes	M
		'9F37'	Unpredictable Number	bytes	M
		'9F02'	Amount, Authorized (Numeric)	bytes	M
		'9F03'	Amount, Other (Numeric)	bytes	O
		'5F2A'	Transaction Currency Code	bytes	M
		'9A'	Transaction Date	bytes	M
		'9C'	Transaction Type	byte	O
		'9F1A'	Terminal Country Code	bytes	O
		'82'	Application Interchange Profile	bytes	M

Figure 11

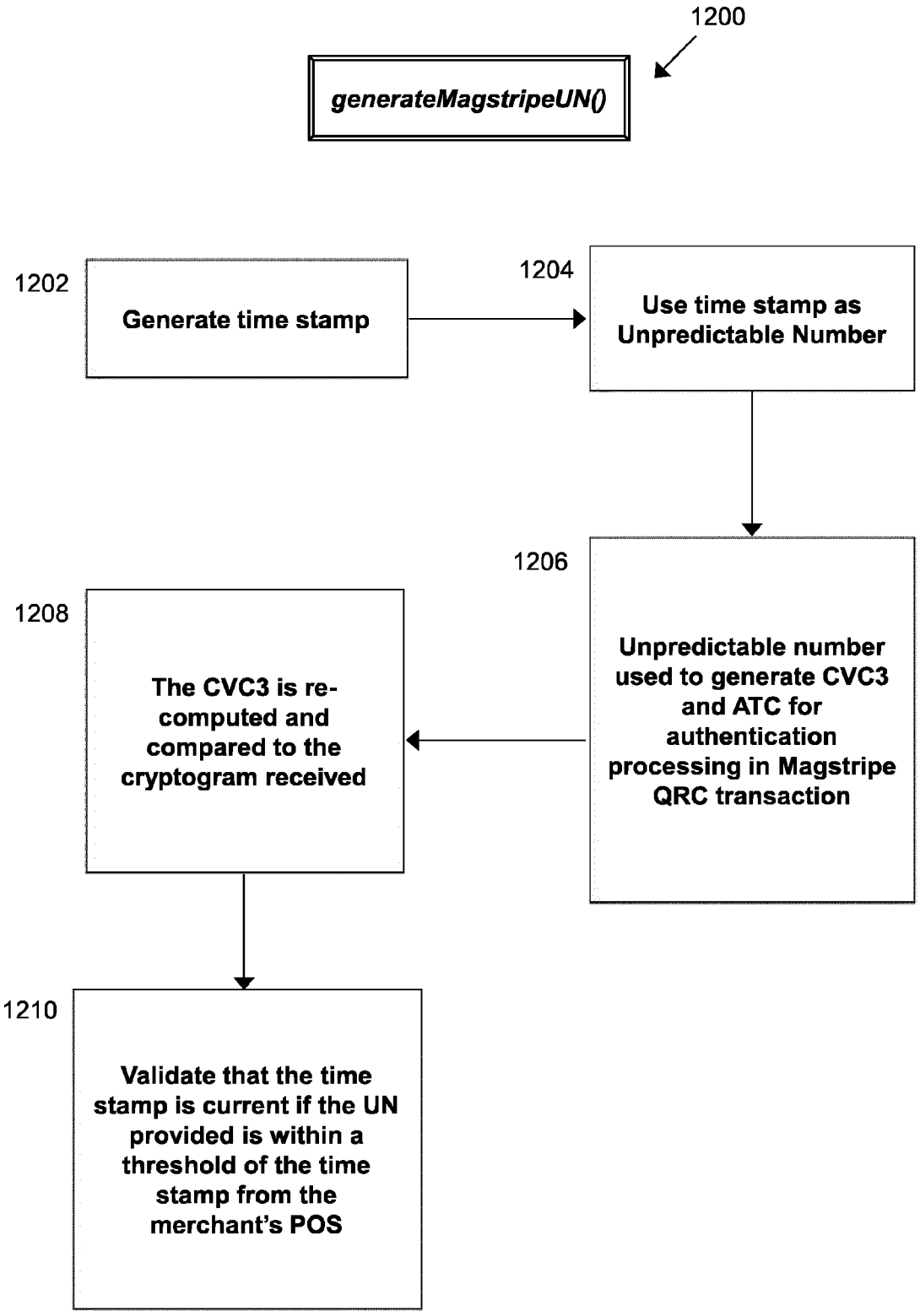

1200
generateMagstripeUN()
1202
Generate time stamp
1204
Use time stamp as Unpredictable Number
1206
Unpredictable number used to generate CVC3 and ATC for authentication processing in Magstripe QRC transaction
1208
The CVC3 is re-computed and compared to the cryptogram received
1210
Validate that the time stamp is current if the UN provided is within a threshold of the time stamp from the merchant's POS

Figure 12

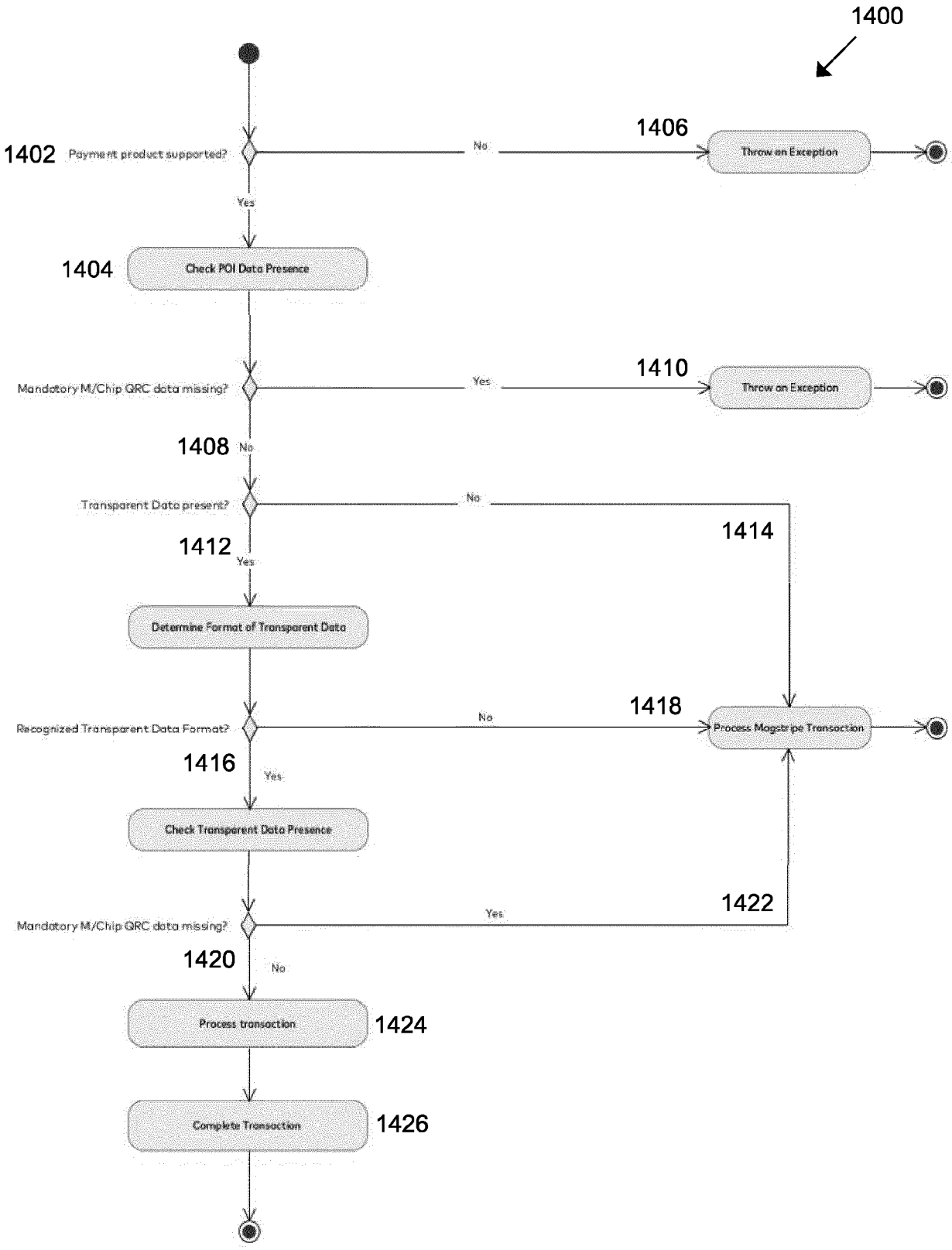
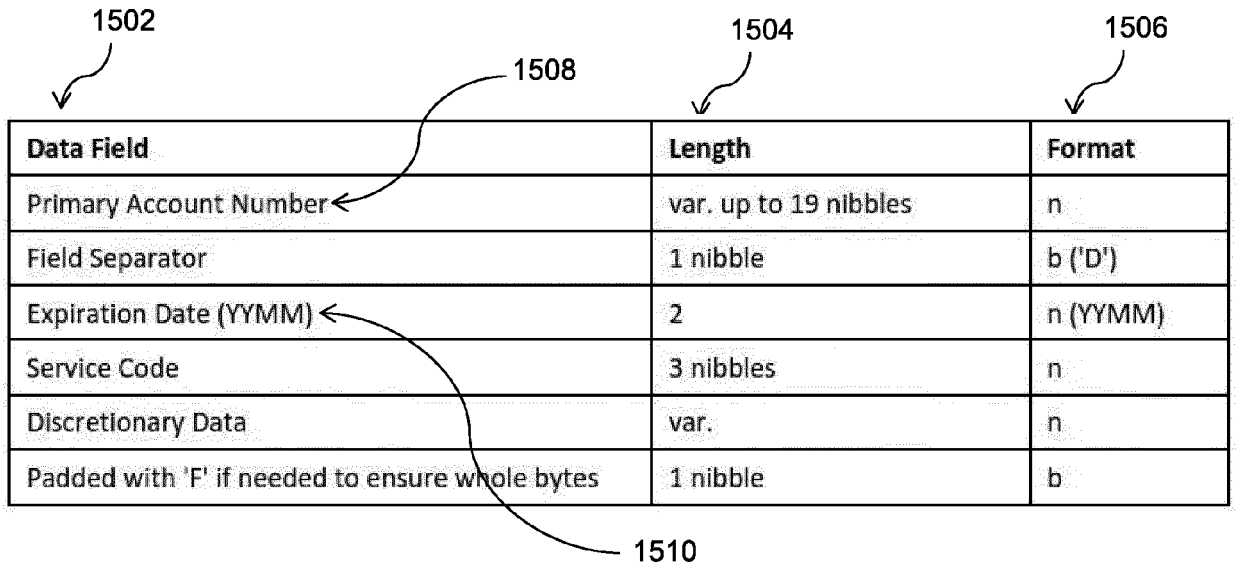

1400
1402
Payment product supported?
No
1406
Throw an Exception
Yes
1404
Check POI Data Presence
Mandatory M/Chip QRC data missing?
Yes
1410
Throw an Exception
1408
No
Transparent Data present?
No
1414
1412
Yes
Determine Format of Transparent Data
Recognized Transparent Data Format?
No
1418
Process Magstripe Transaction
1416
Yes
Check Transparent Data Presence
Mandatory M/Chip QRC data missing?
Yes
1422
1420
No
Process transaction
1424
Complete Transaction
1426

Figure 13



Data Field	Length	Format
Primary Account Number	var. up to 19 nibbles	n
Field Separator	1 nibble	b ('D')
Expiration Date (YYMM)	2	n (YYMM)
Service Code	3 nibbles	n
Discretionary Data	var.	n
Padded with 'F' if needed to ensure whole bytes	1 nibble	b

Figure 14

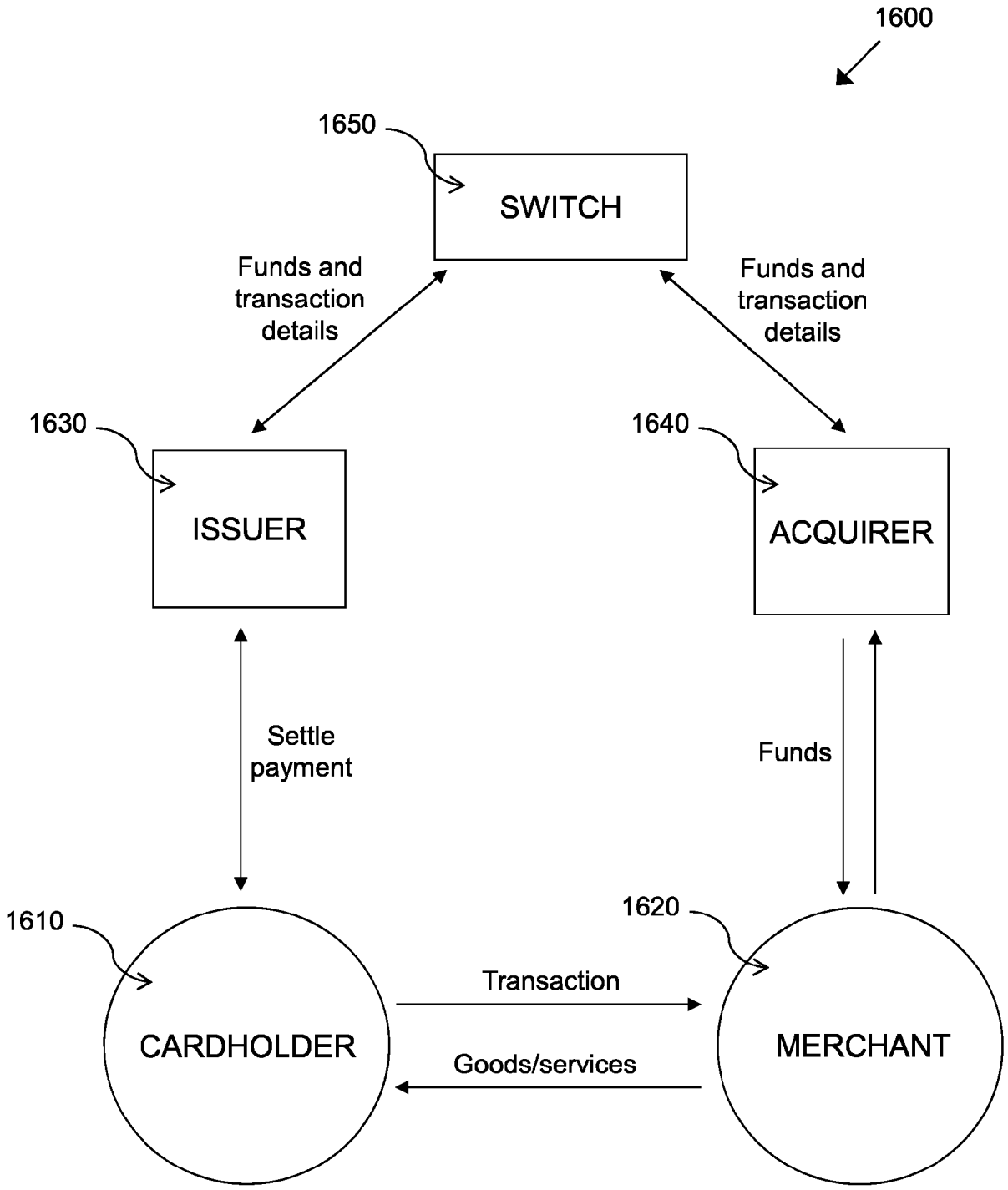

1600
1650
SWITCH
Funds and transaction details
Funds and transaction details
1630
ISSUER
1640
ACQUIRER
Settle payment
Funds
1610
CARDHOLDER
1620
MERCHANT
Transaction
Goods/services

Figure 15

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 17 19 6489

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2014/080353 A1 (BABU SAJAN [IN]; SREEDHARAKURUP SREERAJ [IN]) 30 May 2014 (2014-05-30) * paragraphs [0008], [0040], [0045] - [0051], [0057] - [0058], [0060]; claim 1; figures 1-23, 7, 8 *	1-12	INV. G06Q20/32 G06Q20/36 G06Q20/38
X	US 2007/022058 A1 (LABROU YANNIS [US] ET AL) 25 January 2007 (2007-01-25) * paragraphs [0021] - [0030], [0033], [0044], [0117], [0152], [0160] - [0184] - paragraph [0156]; figures 3-16 *	1-12	
A	US 2015/227922 A1 (FILLER TOMAS [US]) 13 August 2015 (2015-08-13) * the whole document *	1-12	

TECHNICAL FIELDS SEARCHED (IPC)

G06Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	21 February 2018	Guivol, Ouri

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 17 19 6489

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-02-2018

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2014080353 A1	30-05-2014	US 2017154329 A1	01-06-2017
		WO 2014080353 A1	30-05-2014
US 2007022058 A1	25-01-2007	EP 1758053 A1	28-02-2007
		JP 5407104 B2	05-02-2014
		JP 2007042103 A	15-02-2007
		US 2007022058 A1	25-01-2007
US 2015227922 A1	13-08-2015	US 2015227922 A1	13-08-2015
		US 2015227925 A1	13-08-2015
		US 2017024723 A1	26-01-2017

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82